



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09265254 A**(43) Date of publication of application: **07 . 10 . 97**

(51) Int. Cl

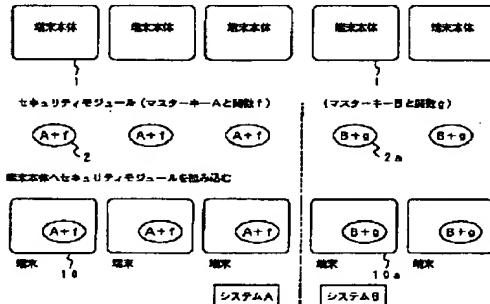
**G09C 1/00**  
**G09C 1/00**  
**G09C 1/00**  
**G06K 19/00**  
**H04L 9/08**  
**H04L 9/10**  
**H04L 9/32**

(21) Application number: **08097410**(22) Date of filing: **28 . 03 . 96**(71) Applicant: **DAINIPPON PRINTING CO LTD**(72) Inventor: **INADA MAYUMI****(54) MUTUAL AUTHENTICATION SYSTEM FOR INFORMATION RECORDING MEDIUM**

## (57) Abstract:

**PROBLEM TO BE SOLVED:** To make a system excellent in security by storing master keys and algorithms needed in operations of mutual authentications by terminals in security modules in readout impossible states to make the keys and the algorithms not to be stolen.

**SOLUTION:** Same terminal main bodies can be used as terminal main bodies 1 even for systems whose users are different. In security modules 2 to be used in a system A, modules in which master keys As and functions (fs) are used are used and in security modules 2a to be used in a system B, modules in which master keys Bs and functions (gs) are used are used for the common main bodies 1. Then, respective terminals 10, 10b for system A, system B can be constituted by building up security modules different in respective systems in common terminal main bodies. Thus, master keys and algorithms are never abused by being decoded illegally from the outside and the high security of this system is kept.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-265254

(43)公開日 平成9年(1997)10月7日

(51) Int.Cl. <sup>6</sup>	識別記号	序内整理番号	F I	技術表示箇所
G 09 C 1/00	6 3 0	7259-5 J	G 09 C 1/00	6 3 0 Z
		7259-5 J		6 3 0 A
	6 4 0	7259-5 J		6 4 0 A
	6 6 0	7259-5 J		6 6 0 A
G 06 K 19/00			G 06 K 19/00	T
			審査請求 未請求 請求項の数 6 FD (全 7 頁) 最終頁に続く	

(21)出願番号 特願平8-97410

(22)出願日 平成8年(1996)3月28日

(71)出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72)発明者 稲田 真弓

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

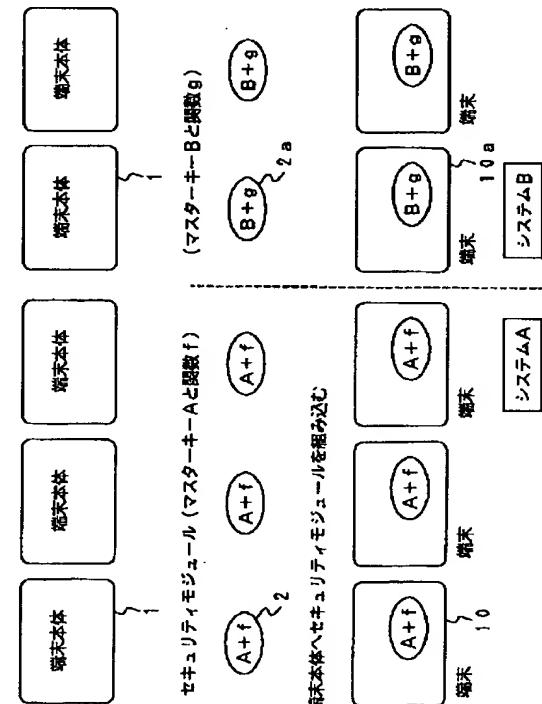
(74)代理人 弁理士 小西 淳美

(54)【発明の名称】 情報記憶媒体の相互認証システム

(57)【要約】

【課題】 端末が相互認証で用いるマスターキー、アルゴリズム等のセキュリティ性を向上し、異なるシステムの端末の製造を容易とする。

【解決手段】 I Cメモリを利用した情報記憶媒体と、情報記憶媒体へのアクセスを行う端末とから、少なくとも構成される、情報記憶媒体の相互認証システムにおいて、端末はセキュリティモジュールを備え、端末が使用するマスターキー並びに個別化キー生成アルゴリズム及び認証アルゴリズムを、このセキュリティモジュールに読み出不可能な状態で内蔵しておく。セキュリティモジュールは、少なくともマスターキーについては書き可能なメモリを備えたマイクロコンピュータを用いて構成し、I Cカード形態とする。



## 【特許請求の範囲】

【請求項1】 ICメモリを利用した情報記憶媒体と、該情報記憶媒体へのアクセスを行う端末とから、少なくとも構成される、情報記憶媒体の相互認証システムにおいて、

端末はセキュリティモジュールを備え、端末が使用するマスターキー、個別化キー生成アルゴリズム及び認証アルゴリズムが、前記セキュリティモジュールに読み出不可状態で内蔵されている、情報記憶媒体の相互認証システム。

【請求項2】 セキュリティモジュールが、少なくともマスターキーについては書き可能なメモリを備えたマイクロコンピュータで構成されている、請求項1記載の情報記憶媒体の相互認証システム。

【請求項3】 セキュリティモジュールは、個別化キー生成アルゴリズムによって生成するワークキーを、該モジュール内部で使用する、請求項2記載の情報記憶媒体の相互認証システム。

【請求項4】 セキュリティモジュールがICカードである、請求項1～3のいずれか1項に記載の相互認証システム。

【請求項5】 情報記憶媒体がICカードである、請求項1～4のいずれか1項に記載の相互認証システム。

【請求項6】 ICカードがプリペイドICカードである請求項5記載の情報記憶媒体の相互認証システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、ICメモリを利用したICカード等の情報記憶媒体と、それに対してアクセスする端末等とからなるシステムで、相互認証を行うシステムに関する。

## 【0002】

【従来の技術】 ICメモリを利用し特にCPUを内蔵したICカードはセキュリティ性に優れ、その一つにCPUの演算処理機能等を用いて相互認証が行える点にある。例えば、電話カード等に試みられているプリペイドICカードシステムでは、端末に挿入されたカードが正当なものであるか否かを端末は確認し、不正なカードの利用を防ぐことが必要である。一方、カードには金額に相当する情報が書き込まれているため、カードに対してアクセスを行う端末が正当なものであるか否かを、カード側でも確認することも必要となる。この両方の確認、すなわち、カード認証（前者）、端末認証（後者）を行うのが相互認証である。

【0003】 相互認証において、端末及びカードのそれぞれに如何なる秘密鍵を持たせるか等は各種の形態があるが、その一つは、カード側に端末認証キー及びカード認証キー及び認証アルゴリズム、さらに乱数生成アルゴリズム等を持たせ、セキュリティ上の観点から端末・カード間ではこれらのキー及びアルゴリズムの伝送を行わず

に、端末側では相互認証に必要なキー及びアルゴリズムを独自に備える形態がある。例えば、端末には、マスターキーと個別化キー生成アルゴリズムとを持たせ、これに認証の都度カードから取得したカードIDとを用いて、ワークキーとして端末認証キー及びカード認証キーを生成する。また、端末側にもカードが所有しているのと同一の認証アルゴリズムを持たせておき、端末は上記で得た認証キーとこの認証アルゴリズムとを用いて（さらに、カード認証の場合には、端末が備えた乱数生成アルゴリズムも用いる。）、認証を行う形態である。

【0004】 ところが、端末において、これら①マスターキー、②個別化キー生成アルゴリズム、及び③認証アルゴリズムの、従来の格納方法としは、アルゴリズム②及び③は端末制御用プログラムに組み込んでおく形態、マスターキー①は制御用プログラムから任意にアクセス可能な端末のメモリに書き込んでおく形態等が採られていた。

## 【0005】

【発明が解決しようとする課題】 ところが、マスターキー等が任意にアクセス可能なメモリ中に格納されていると、端末制御のプログラムを知っている者によって読み出されてしまう恐れがあるという問題点があった。また、このマスターキー及びアルゴリズムは、カードシステムを運営するユーザ毎、或いはシステム毎に変える必要があり、システムの製造者として多くのユーザーに対応するためには、各々異なる端末制御用プログラムを製作して組み込むことが必要となるという問題点があった。

また、この他、システム運用後にマスターキー及びアルゴリズムを変更する必要が生じた場合に、端末そのものを変更しなければならないという問題点もあった。

## 【0006】

【課題を解決するための手段】 そこで上記課題を解決する為に、本発明の情報記憶媒体の相互認証システムでは、端末側に独自に格納しておく、マスターキー、並びに、個別化キー生成アルゴリズム及び認証アルゴリズムを、セキュリティモジュールという端末本体とは別のモジュール、例えばICカードに格納する形態とし、しかもこのセキュリティモジュールは少なくともマスターキーは書き込むことが可能なマイクロコンピュータを用いて構成した。格納されたこれらの内容は外部から読み出不能な状態で格納しておき、また個別化キー生成アルゴリズムで生成したワークキーである端末認証キー及びカード認証キーはセキュリティモジュール外部に出さずに該モジュール内のみで使用し、端末本体側ではこれらを用いた演算結果をセキュリティモジュールから取得する様にして相互認証に利用する構成とする。この結果、マスターキー及びアルゴリズムが外部から不正に解読されて悪用されることなく、高いセキュリティ性を保つことができる。

また、汎用的に同一の制御プログラムを有する端末本体を製造しておき、ユーザやシステムに応じたマスター

キーと個別化キー生成及び認証の為のアルゴリズムが格納されたセキュリティモジュールを端末本体に組み込むことにより端末とするために、効率的にユーザー毎やシステム毎のマスターキーとアルゴリズムを管理できることとなる。

### 【0007】

【発明の実施の形態】以下、図面を参照しながら本発明の情報記憶媒体の相互認証システムを説明する。本発明のシステムは情報記憶媒体としてICカードと端末との関係に限定されるシステムではないが、ここでは、ICカードと端末との相互認証を想定して以下説明する。図1は本発明の相互認証システムにおける、図2は従来の相互認証システムにおける、端末が保有する、マスターキー及びアルゴリズムの格納状態を対比した概念図である。図1及び図2においては、「A」はマスターキーAを、「B」はマスターキーBを表し、また、アルゴリズムとしてfは関数fを、gは関数gを表す。先ず、図1に示す本発明の情報記憶媒体の相互認証システムでは、端末本体1としては、ユーザが異なるシステムに対しても、全て同一の端末本体を用いることができる。この共通の端末本体1に対して、システムAに用いるセキュリティモジュール2にはマスターキーA及び関数fが格納されているものを、システムBに用いるセキュリティモジュール2aにはマスターキーB及び関数gが格納しているものを用いる。そして、前記共通の端末本体に上記各システムで異なるセキュリティモジュールを組み込むことによって、システムA、システムB用のそれぞれの端末10及び10aを構成することができる。

【0008】次に、図2は従来の情報記憶媒体の相互認証システムにおける端末の一例を示す概念図であり、セキュリティモジュールを備えておらず、マスターキーや関数等は、システムA及びシステムB用のそれぞれの端末10b及び10cとは分離独立可能な形態ではなく、端末10b、10cと不可分の関係で端末に組み込まれている。端末10b、10cに備える制御プログラムに、個別キー生成アルゴリズム及び認証アルゴリズムが組み込まれ、また端末が備えるメモリにマスターキーが格納されている。システムAにおける端末10bには、マスターキーA及びシステムA用の関数(図示せず)、同様にシステムBにはマスターキーB及びシステムB用の関数(図示せず)が格納されて、端末10cとなる。なお、図では便宜上、各システムは、一つのマスターキーA又はBと、一つの関数f又はgとを備えているかの如く表現されているが、本発明のシステムでは、マスターキーは一つとは限らず、端末認証キー生成用とカード認証キー生成用とでそれぞれ独立の異なるマスターキーを備えている場合も意味する。また、関数、すなわちアルゴリズムは、個別キー生成アルゴリズム及び認証アルゴリズムの両方を備えていることを意味する。また、個別化キー生成アルゴリズムは、端末認証キー及びカード

(情報記憶媒体)認証キー生成で共通の同一のもの、或いは別個のものでも良い。

【0009】このように本発明の情報記憶媒体の相互認証システムは、従来の相互認証システムに対して、少なくともマスターキー、認証キー生成アルゴリズム及び認証アルゴリズムをモジュール化して、その他の部分を端末本体1として、端末本体1とセキュリティモジュール2とから端末10を構成し、しかもセキュリティモジュールに格納したマスターキーとアルゴリズムは、該モジュールの外部からは読み取ることができない様にしたものである。

【0010】そして、マスターキー並びに個別化キー生成アルゴリズム及び認証アルゴリズムは、セキュリティモジュールに読み出不可能な状態で格納される。マスターキーは、セキュリティモジュールが備えるメモリに格納するが、これは例えばセキュリティモジュールをマイクロコンピュータを用いて構成することで、前記マスターキーを格納するメモリを該マイクロコンピュータの制御下に置き、マスターキーへのアクセスの属性を読み出禁止属性とすることで達成される。このマスターキーについてはさらに書き込み可能な属性としておけば、システム運用後にマスターキー変更の必要性が生じた場合に、セキュリティモジュールを使い捨てにせずにマスターキーを容易に変更することもできる。或いは、不正に書き換えられない様に、一旦マスターキーの書き込みを行ったならば、ファイル属性で或いは物理的に書き込み禁止にしておいても良い。また、個別化キー生成アルゴリズムや認証アルゴリズムは、このマイクロコンピュータの実行プログラムとして前記メモリ等に読み出禁止属性を付けて書き込んで置いても良いし、また、各アルゴリズム専用の演算回路(算術論理ユニット:ALU)として組み込んで良い。また、認証に用いる乱数を得る為の、乱数発生アルゴリズムの格納も行う場合は、マイクロコンピュータの実行プログラムとして組み込んで良いし、或いは演算回路として組み込んでよい。なお、マスターキーを格納するメモリはCPUと共に1チップ化したメモリ、或いは別チップのメモリでも良い。また、上記の演算回路もCPU、メモリ等とともに1チップ化したマイクロコンピュータを用いても良い。

【0011】上記の様な、セキュリティモジュールの物理的形態は、例えばICカード等のカード状の形態、或いは携帯電話の一部で実用化されているSIM(Sub subscriber Identity Module)等のICチップ等の形態である。カードとすることで、端末本体とは容易に分離独立させて、端末とは別のセキュリティ性の管理された所で、セキュリティモジュールにマスターキーの設定を行ったり、各ユーザ毎の或いは各システム毎のセキュリティモジュールの製造、或いは設定の変更を安全に行えることが可能となる。この様にカード形態の場合、容易に端末本体への組込み及び脱着が

できるが、本発明のセキュリティモジュールはカード以外の形態でも良い。セキュリティモジュールの上記機能は、1チップ或いは数チップのICによって実現できるので、これらを1パッケージとしてまとめたICとしても良く、端末本体のICソケットに実装することで、セキュリティモジュールを端末本体から脱着可能に組み込むことができる。なお、本発明では、セキュリティモジュールは必ずしも脱着可能に分立独立できる形態で端末本体に組み込むことは必要ではない。

【0012】次に、上記セキュリティモジュールに読み出不可能な状態で内蔵されている、マスターキー並びに個別化キー生成アルゴリズム及び認証アルゴリズム、さらに適宜乱数発生アルゴリズムは、それらを該モジュールから解読されることなく、それらを用いた演算結果のみが端末本体側に読み出されて認証に使用される。端末はカードID（情報記憶媒体の識別情報）をカードから取得し、これとマスターキーと個別化キー生成アルゴリズムを用いて、カードが保有する端末認証キーやカード認証キーを生成するが、さらに、セキュリティモジュールのマイクロコンピュータにより、この各認証キーもセキュリティモジュールから読み出されることなく該モジュール内で使用してその使用結果のみを端末本体側では読み出すことが出来る様にすれば、ワークキーである認証キーに対するセキュリティ性も向上する。

【0013】そして、以上のようなセキュリティモジュールを備えた端末を用いる、本発明の情報記憶媒体の相互認証システムのシステム全体としては、情報記憶媒体には従来公知の相互認証機能を有するICカード等が使用でき、通常は複数の端末がホストコンピュータに接続されたシステムとして構成される。相互認証機能を有するICカードは、ICメモリ以外にCPU等を備えたマイクロコンピュータ等を備えることで相互認証機能を実行する。なお、ICメモリ以外に光メモリ等の光学記録メモリ、磁気メモリ等を備えていても良い。また、情報記憶媒体のICカードがプリペイドICカードであれば、プリペイドICカードシステムとなり、情報記憶媒体をICカードとすれば、その使い方によって各種用途に適した、相互認証機能を有するICカードシステムとなる。

#### 【0014】

【実施例】次に、本発明の情報記憶媒体の相互認証システムの一実施例としてICカードシステムを説明する。図3は本システムの一実施例における端末10について、そのセキュリティモジュール2の概略構成図である。同図のシステムの端末10は、従来の相互認証システム機能を有するICカードシステムの端末において、少なくともマスターキー、認証キー生成アルゴリズム及び認証アルゴリズムを、ICカード形態のモジュールとして、その他の部分を端末本体1として、端末本体1とセキュリティモジュール2とから端末10を構成し、し

かもセキュリティモジュールに格納したマスターキー及びアルゴリズム、さらに得られる認証キーも、該モジュールの外部からは読み取ることができない様に、マイクロコンピュータで制御したものである。また、システム全体としては、情報記憶媒体はICメモリとCPUを内蔵し相互認証機能を有するICカードを使用し、通常は複数の端末がホストコンピュータに接続されたシステムとして構成される。なお、このICカードをプリペイドICカードとすれば、プリペイドICカードシステムとなる。

【0015】図3に示すセキュリティモジュール2は、マイクロコンピュータ3と、個別化キー生成アルゴリズム及び認証アルゴリズムをおのおの演算する暗号回路6、認証に用いる乱数を発生する乱数発生アルゴリズムを演算する乱数発生回路7とを備える。また、マイクロコンピュータ(MPU)3は、中央演算処理装置であるCPU4とメモリ5とが1チップのLSIとなっており、メモリ5にはCPUが実行する各種プログラム、マスターキー等が格納され、また作業用メモリもこの中に確保されている。同図の様にメモリへのアクセスはCPUを通してアクセス可能であり、マスターキーは、例えば読み出禁止属性を有するファイル等としての形態で、外部から読み出不可能な状態で、セキュリティモジュールに格納されている。また、マスターキー及び個別化キー生成アルゴリズムを用いて生成される端末認証キー及びカード認証キーの認証キーは、セキュリティモジュール内でのみ使用される。

【0016】そして、メモリ5に端末認証用として（後述する）マスターキーA1を、カード認証用としてマスターキーA2が格納され、暗号回路6は、端末認証キー及びカード認証キーの生成に用いる個別化キー生成アルゴリズムとして関数gを、認証アルゴリズムとして関数fを演算し、乱数発生回路7は、（後述する）乱数（関数）Bを演算し、そして、マイクロコンピュータ3はこれらを用いて、認証の為の照合用データを作成し、端末本体側へ返す。

【0017】次に、図4の端末認証、図5のカード認証のフロー図を参照しながら本発明の情報記憶媒体の相互認証システムによる認証のフローを説明する。

【0018】図4で、左側はICカード側の処理を、右側は端末内のセキュリティモジュール内の処理を示す。端末本体（以下、単に端末）は認証に必要なICカードとセキュリティモジュールとのデータの受渡しを行う。ICカードが端末を認証する端末認証のフローでは、まず、端末はICカードから端末認証用の「カードID1」を読み取り、これを端末内のセキュリティモジュールに渡す（ステップS1、以下S1等と記す）。そして、セキュリティモジュールでは上記「カードID1」と該モジュールに格納された「マスターキーA1」とから個別化キー生成アルゴリズムである関数gを用いて、

端末認証用のワークキーである「認証キー1 g (ID 1)」を生成する (S 2)。次に、端末は IC カードの乱数 (関数) A で発生させた「乱数RNA」を読み取りセキュリティモジュールに渡す (S 3)。そして、セキュリティモジュールは、前記生成済みの「認証キー1 g (ID 1)」と上記「乱数RNA」とから認証アルゴリズムである関数 f を用いて「照合用データ f (g (ID 1)、RNA)」生成する (S 4)。次に、端末はセキュリティモジュールで生成済みの「照合用データ f (g (ID 1)、RNA)」を IC カードに伝送する (S 5)。一方、IC カード側では、上記「照合用データ f (g (ID 1)、RNA)」が IC カード内で生成する照合用データと同一であるかを比較するための以下の処理を行う。IC カードは、IC カードの乱数 (関数) A で発生させ前記で端末に伝送したものと同一の「乱数RNA」と、IC カード内に格納されている端末認証用の「認証キー1 (g (ID 1))」とから (IC カードに格納されている) 関数 f を用いて、「照合用データ f (g (ID 1)、RNA)」生成する (S 6)。そして、IC カードのこの自己生成した照合用データと、端末側で生成した照合用データとを比較する (S 7)。一致している場合は IC カードは端末を正しいものと認証とする。

【0019】次は、図 5 で、端末が IC カードを認証するカード認証のフローを説明する。先ず、端末は IC カードからカード認証用の「カード ID 2」を読み取り、これを端末内のセキュリティモジュールを渡す (ステップ S 11)。そして、セキュリティモジュールでは上記「カード ID 2」と該モジュールに格納されたカード認証用のマスターキーである「マスターキー A 2」とから関数 g を用いて、カード認証用の「認証キー2 g (ID 2)」を生成する (S 12)。次に、端末はセキュリティモジュールに格納された乱数 (関数) B で発生させた「乱数RNB」を IC カードに伝送する。そして、IC カードは自己が保有する「認証キー2 g (ID 2)」と上記「乱数RNB」とから (自己が保有する) 関数 f を用いて「照合用データ f (g (ID 2)、RNB)」生成する (S 14)。次に、端末はこの「照合用データ f (g (ID 2)、RNB)」を IC カードから読み出し、セキュリティモジュールに渡す (S 15)。また、端末側では、上記「照合用データ f (g (ID 2)、RNB)」が端末内で生成する照合用データと同一であるかを比較するための以下の処理を行う。端末のセキュリティモジュールは、その乱数 (関数) B で発生させ前記で IC カードに伝送したのと同一の「乱数RNB」と、前記ステップ S 12 で生成した「認証キー2 (g (ID 2))」とから (セキュリティモジュールに格納されている) 関数 f を用いて、「照合用データ f (g (ID 2)、RNB)」生成する (S 6)。そして、セキュリティモジュールはこの自己生成した照合用データと、I

C カード側で生成した照合用データとを比較する (S 17)。一致している場合は端末は IC カードを正しいものと認証とする。以上の様にして、端末認証及びカード認証が行われる。

【0020】なお、本発明の情報記憶媒体の相互認証システムは、上記実施例に限定されず、前述の如く各種形態があり得る。例えば、上記実施例の相互認証では、端末認証キー及びカード認証キーの生成に異なるカード ID を用いたが、各認証キーで同一のカード ID を用いる等である。また、情報記憶媒体としての IC カードは、その用途により、クレジットカード、バンクカード、プリペイドカード等の多様である。

#### 【0021】

【発明の効果】端末が相互認証の演算に必要とする、マスターキー及びアルゴリズムがセキュリティモジュール内に格納され、その演算と演算の途中結果を外部から読み出すことが不可能であり、キーとアルゴリズムを盗み出すことができず、セキュリティ性に優れる。セキュリティモジュールに格納するマスターキーを、マイクロコンピュータによって読み出不能且つ書き可能に制御されたメモリに格納することで、マスターキーはセキュリティ性を保った上で、マスターキーの途中での変更もできる。また、マスターキーとこれらアルゴリズムを、端末本体と切り離した状態でセキュリティモジュールで設定ができるため、ユーザー毎やシステム毎の管理が行いやすい。また、マスターキーとこれらアルゴリズムを、変更する必要が生じた場合に、セキュリティモジュールのみを交換するだけで、容易に変更ができる。

#### 【図面の簡単な説明】

【図1】本発明の情報記憶媒体の相互認証システムにおける端末の概念図。

【図2】従来の情報記憶媒体の相互認証システムにおける端末の概念図。

【図3】本発明の相互認証システムの一実施例である IC カードシステムでの端末のセキュリティモジュールを中心とした概略構成図。

【図4】本発明における端末認証処理の一例を示すフロー図。

【図5】本発明におけるカード認証処理の一例を示すフロー図。

#### 【符号の説明】

1 端末本体

2、2 a セキュリティモジュール

3 MPU

4 CPU

5 メモリ

6 暗号回路

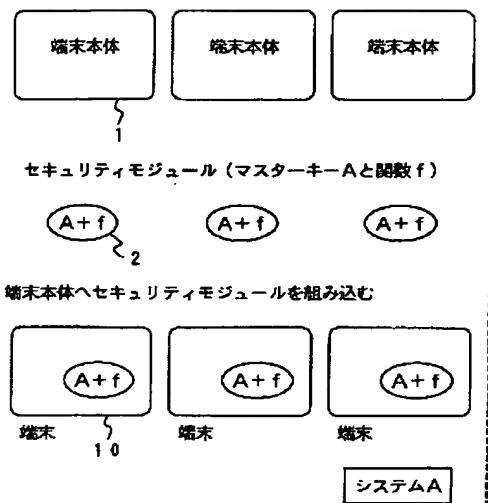
7 乱数発生回路

10、10 a～10 c 端末

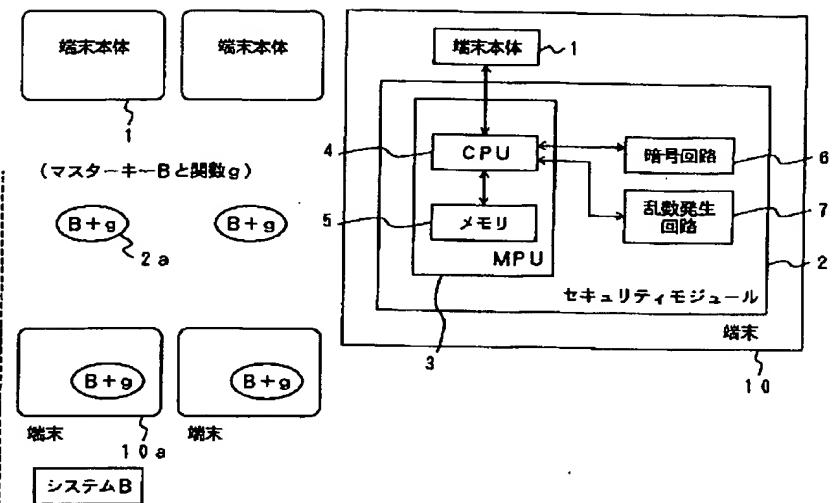
A、A 1、A 2、B、B 1、B 2 マスターキー

f, g 関数、アルゴリズム

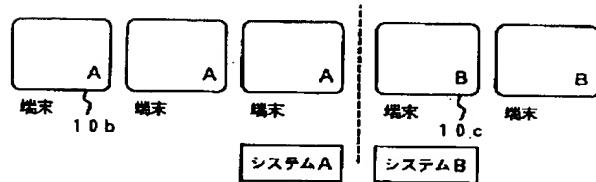
【図1】



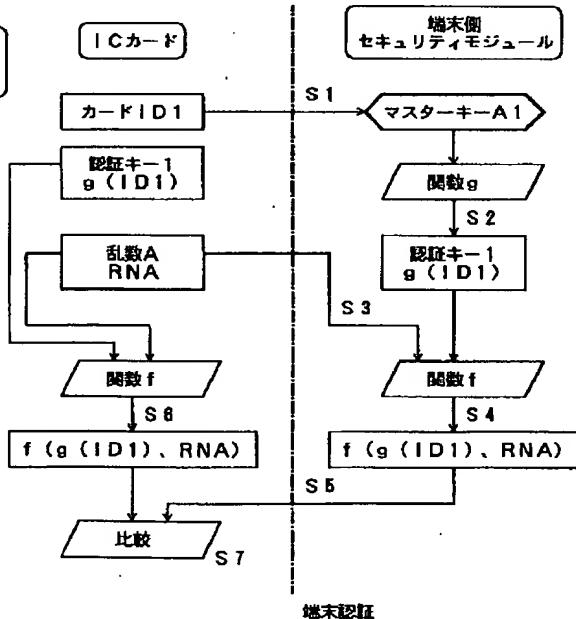
【図3】



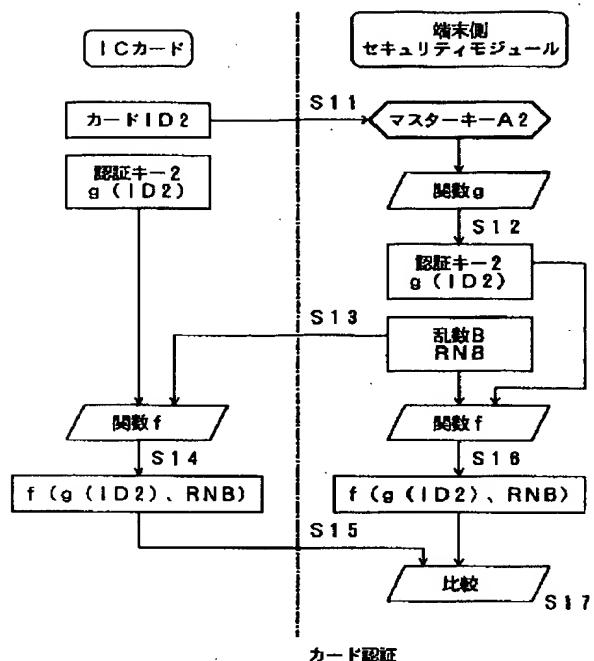
【図2】



【図4】



【図5】



フロントページの続き

(51) Int. Cl. <sup>6</sup>	識別記号	府内整理番号	F I	技術表示箇所
H 0 4 L	9/08		H 0 4 L 9/00	6 0 1 A
	9/10			6 2 1 A
	9/32			6 7 5 A